**Michael J. Gayan**
Claggett & Sykes Law Firm
4101 Meadows Lane, Suite 100
Las Vegas, Nevada 89107
Tel. (702) 655-2346
mike@claggettlaw.com

**John A. Yanchunis**
Morgan & Morgan
Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. (813) 223-5505
jyanchunis@ForThePeople.com

**Douglas J. McNamara**
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW
8th Floor
Washington, D.C. 20005
Tel. (202) 408-4600
dmcnamara@cohenmilstein.com

**Amy Keller**
DiCello Levitt LLP
10 North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Tel. (312) 214-7900
akeller@dicellolevitt.com

*Counsel for Plaintiffs and the Proposed Classes*

*(Additional Counsel Listed on Signature Page)*

**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEVADA**

Dhaman Gill, April Elvidge, Carey Hylton, Charles Popp, Crystal Brewster, Cynthia Rubner, Isaac Dwek, John Gedwill, Laura McNichols, Thomas McNichols, Miguel Rodriguez, Virginia Stacy, William Rubner, and Edward Cherveny, on behalf of themselves and all others similarly situated,

PLAINTIFFS,

v.

Coforge, Inc., and Coforge, Ltd.,

DEFENDANTS

Master File No. 2:23-cv-01447-ART-BNW
Filing relates to No. 2:25-cv-00736

**AMENDED CLASS ACTION COMPLAINT**

**TABLE OF CONTENTS**

Plaintiffs Dhaman Gill, April Elvidge, Carey Hylton, Charles Popp, Crystal Brewster, Cynthia Rubner, Isaac Dwek, John Gedwill, Laura McNichols, Thomas McNichols, Miguel Rodriguez, Virginia Stacy, William Rubner, and Edward Cherveny ("Plaintiffs") bring this Amended Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Defendants Coforge, Inc. and Coforge, Ltd. (collectively "Coforge" or "Defendants") (formerly NIIT Technologies Ltd.) alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs.

## I. INTRODUCTION

1. This is a class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a cyberattack on Caesars Entertainment, Inc. ("Caesars") and Coforge on or around August 23, 2023 (the "Data Breach"). Plaintiffs have already sued Caesars over its failure to protect their data. *See In re Data Breach Sec. Litig. Against Caesars Entertainment, Inc.*, 2:23-cv-01447-ART-BNW (D. Nev.).

2. Through the early investigations in that case, Plaintiffs' counsel has learned Coforge provided "service desk" services and acted as a Caesars' third-party IT vendor at the time of the Data Breach. One task for Coforge was to handle password support including resetting passwords and unlocking Caesars' employees' accounts. However, due to apparent inadequate safeguards and poor training, Coforge allowed the cybercriminals to carry out a successful "vishing" attack, granting a password reset to a caller impersonating an internal Caesars employee allowing access Caesars' network without verifying the caller's identity.[1] Then, due to Coforge's actions, those attackers spent five days within Caesars' network, undetected, before copying and exfiltrating the personally identifiable information ("PII").

3. According to Caesars, it has one of the largest loyalty programs in the gaming industry, with over 65 million members.[2] Caesars has also stated it has the "largest and most

[1] A "vishing" attack is a cybercrime that involves using phone calls or voice messages to trick people into giving away sensitive information Univ Info. Security Office, *Phishing, Smishing, and Vishing..Oh My!*, Georgetown Univ. (last accessed March 25, 2025), https://security.georgetown.edu/csam-2020/phishing-smishing-and-vishing-oh-my/.

[2] Caesars Entertainment, *Caesars Entertainment's Loyalty Program, Caesars Rewards®, Wins for*

diversified collection of gaming destinations in the U.S." and considers itself a "global leader in gaming and hospitality."[3] Based on available information and belief, the Data Breach involves tens of millions of its customers' PII. Individuals, including Plaintiffs and Class Members, were customers of Caesars' gaming and entertainment services and/or members of Caesars' Rewards program.

4. While Caesars has not publicly disclosed the exact number of individuals impacted by the Data Breach, it has confirmed that the cybercriminals were able to obtain a copy of Caesars' loyalty program database, including the driver's license numbers and Social Security numbers for a "significant number" of its more than 65 million program members.[4] Caesars' Form 8K disclosed that the breach even went beyond a copy of the loyalty program database, providing "[a]s a result of our investigation, on September 7, 2023, we determined that the unauthorized actor acquired a copy of, *among other data*, our loyalty program database."[5]

5. According to reports, the cyberattack that led to the Data Breach was conducted by a cybercriminal organization known as Scattered Spider, which specializes in gaining access credentials to a target's data systems by impersonating people in the organization through convincing phone calls.[6]

---

*"Best Customer Service" and "Best Promotion" at Prestigious Freddie Awards on April 21* (Apr. 22, 2022), https://investor.caesars.com/news-releases/news-release-details/caesars-entertainments-loyalty-program-caesars-rewardsr-wins.

[3] Caesars Entertainment, *Caesars Company Snapshot*, https://newsroom.caesars.com/overview/default.aspx (accessed Apr. 7, 2025).

[4] Zack Whittaker, *Caesar's Entertainment says customer data stolen in cyberattack*, TechCrunch (Sept. 14, 2023), https://techcrunch.com/2023/09/14/caesars-entertainment-data-breach-cyberattack/; Caesars Entertainment, *Caesars Entertainment's Loyalty Program, Caesars Rewards®, Wins for "Best Customer Service" and "Best Promotion" at Prestigious Freddie Awards on April 21* (Apr. 22, 2022), https://investor.caesars.com/news-releases/news-release-details/caesars-entertainments-loyalty-program-caesars-rewardsr-wins. *See also* Caesars Entertainment, *Caesars Informational Website*, IDX (now removed), web.archive.org/web/20230914191948/https://response.idx.us/caesars/.

[5] *See* Caesars Entertainment, Inc. Form 8-K, Report of unscheduled material events or corporate event, at 2 (Sept. 14, 2023), *available at* https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57.

[6] Sara Morrison, *The chaotic and cinematic MGM casino hack, explained*, Vox (Oct. 6, 2023), https://www.vox.com/technology/2023/9/15/23875113/Caesars-hack-casino-vishing-cybersecurity-ransomware.

6. Coforge's responsibilities were set out in a Statement of Work ("SOW") under its contract with Caesars that limited whom Coforge could give access to Caesars' customers' sensitive personal information, including government issued identification numbers. The SOW explained to Coforge the importance of the data and the risks of it being unlawfully accessed, requiring Coforge to perform background checks on those who could access the data; to encrypt transmitted data; immediately inform Caesars of any suspicions of unauthorized access; cover the costs of any security breach; and carry sufficient insurance to address the cybersecurity risks.

7. A vishing attack was eminently foreseeable. Plaintiffs and Class Members were the foreseeable and probable victims of Coforge's failure to prevent such an intrusion. Coforge assumed legal and equitable duties to Plaintiffs and Class Members to safeguard that information and knew, or should have known, it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure. Plaintiffs and Class Members had a reasonable expectation that appropriate safeguards would be employed to protect their PII. Coforge had unreasonable safeguards in place, leading to the Data Breach.

8. Upon information and belief, Coforge's ineptitude, recklessness, and gross negligence allowed the cybercriminals to bypass standard data security safeguards, such as not verifying phony Caesars employee's identity in the vishing attack, and enter the Caesars network.

9. After gaining access to Caesars' systems through the facile attack on Coforge, the cybercriminals extracted the loyalty member database and demanded Caesars pay a $30 million ransom.[7] According to reports, Caesars *agreed* to pay roughly half of the ransom demand to the hackers.[8] Even if true, and the payment were *actually* made, that payment has done little to protect the PII or mitigate the resulting harm of Plaintiffs and Class Members, many of whom have already experienced fraud or attempted fraud or received notification that the exact data Coforge failed to protect has been found on the dark web. Caesars has acknowledged that, while it had taken steps

[7] Rohnan Goswami & Contessa Brewer, *Caesars paid millions in ransom to cybercrime group prior to MGM hack*, CNBC (Sept. 14, 2023), https://www.cnbc.com/2023/09/14/caesars-paid-millions-in-ransom-to-cybercrime-group-prior-to-mgm-hack.html.

[8] *Id.*

to have the stolen data erased by the cybercriminals, it could not "guarantee" that that data was, in fact, erased or not shared before it was erased.[9]

10. If Caesars held the keys to its own databases, Coforge was the locksmith. Coforge had the ability to provide anyone unfettered access to that PII that readily enables identity theft—so it is reasonably foreseeable that, if Coforge gave access to unauthorized third parties, Plaintiffs and Class Members would be injured. Yet, despite knowing of the serious risk of cyberattack faced by the gaming and hospitality industry, Coforge operated Caesars' service desk in a negligent and reckless manner, which left Plaintiffs and Class Members' PII vulnerable to theft and unlawful use.

11. The Data Breach resulted in part from Coforge's failure to implement reasonable IT security measures to protect Class Members' PII against unauthorized intrusions and access. Its conduct here was unconscionable.

12. As a result of the Data Breach, Plaintiffs and Class Members have been damaged in several ways. Plaintiffs and Class Members have endured actual and attempted fraud and/or have been exposed to an increased risk of fraud, identity theft, and other misuse of their PII. Plaintiffs and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. To protect

[9] Amaris Encinas, *Caesars Entertainment ransomware attack targeting loyalty members revealed in SEC filing*, USA Today (Sept. 14, 2023), https://www.usatoday.com/story/tech/news/2023/09/14/caesars-entertainment-cyberattack-loyalty-members-data-breach/70856343007/; Caesars' Sample Data Breach Notice, https://attorneygeneral.delaware.gov/wp-content/uploads/sites/50/2023/10/Caesars-AG-Notice-Sample-Notice.pdf. (last visited July 26, 2024). *See also* Lawrence Adams, *Scam PSA: Ransomware gangs don't always delete stolen data when paid*, BleepingComputer (Nov. 4, 2020), https://www.bleepingcomputer.com/news/security/scam-psa-ransomware-gangs-dont-always-delete-stolen-data-when-paid/ ("Companies should automatically assume that their data has been shared among multiple threat actors and that it will be used or leaked in some manner in the future, regardless of whether they paid."); Mathew J. Schwartz, *Ransom Realpolitik: Paying for Data Deletion Is for Suckers*, Bank Info Security (Dec. 1, 2022), https://www.bankinfosecurity.com/ransom-realpolitik-paying-for-data-deletion-for-suckers-a-20596 ("[U]rges victims to never pay for any promise or guarantees to delete data, including for victims in the healthcare sector that might be trying to minimize any impact on patients"); Bill Toulas, *Ransom payments fall as fewer victims choose to pay hackers*, BleepingComputer (July 28, 2022), https://www.bleepingcomputer.com/news/security/ransom-payments-fall-as-fewer-victims-choose-to-pay-hackers/ ("Coveware underlines that in many cases, despite receiving the ransom payment, the threat actors continued the extortion or leaked the stolen files anyway.").

themselves from this increased risk of fraud, Plaintiffs and Class Members will be forced to take proactive measures to mitigate against identity theft, including but not limited to purchasing credit monitoring and other identity protection services, purchase credit reports, place credit freezes and fraud alerts on their credit reports, and spend time investigating and disputing fraudulent or suspicious activity on their accounts and potentially with the Internal Revenue Service given the exposure of Social Security numbers. Plaintiffs and Class Members also did not choose to share their information with unauthorized third parties, so they have lost the economic value of negotiating a fair price for their PII because of the Data Breach.

13. PII stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources (such as publicly available information, social media, etc.) to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen PII to send spear-phishing emails and text messages to Class Members to trick them into revealing even more sensitive information than that which was already exposed—leading to full account takeovers, financial fraud, and life-altering identity theft. Thieves can also send emails and text messages embedded with ransomware.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated consumers whose PII was stolen in the Data Breach. Plaintiffs seek remedies including: (i) compensation for the theft and misuse of their data; (ii) reimbursement of out-of-pocket costs; (iii) compensation for time spent responding to the Data Breach; and (iv) damages consisting of the lifetime cost of comprehensive identity protection services.

## II. PARTIES

### A. Plaintiffs

#### 1. California Plaintiffs

15. Plaintiff **Dhaman Gill** ("Plaintiff Gill") is a citizen and resident of the state of California. Plaintiff Gill has been a Caesars Reward member during the relevant time period. Plaintiff Gill regularly gambled with Caesars in person and stayed at Caesars resorts, at which time Caesars regularly collected his PII.

16. To obtain his membership, Plaintiff Gill was required to provide Caesars with his

PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Gill was required to provide to obtain his Caesars Rewards membership.

17. On October 11, 2023, Plaintiff Gill learned of the Data Breach from an email received from Caesars. Shortly thereafter in October 2023, Plaintiff Gill learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

18. Plaintiff Gill has been careful to protect and monitor his identity. After the Data Breach, Plaintiff Gill purchased his own credit monitoring service (Experian Identity Works) for an annual fee of $400.

19. As a result of the Data Breach, Plaintiff Gill made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: contacting his credit card companies to change cards, contacting his phone company to activate a "spam blocker," purchasing credit monitoring services for $400 per year, monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received 3-5 times every day since the Data Breach. Plaintiff Gill has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

20. Despite these efforts, Plaintiff Gill suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory

damages; and (xi) the continued and certainly increased risk of identity theft and fraud.

21. In addition, as a result of the Data Breach, Plaintiff Gill has experienced multiple attempts of identity theft and fraudulent activity regarding his credit card accounts, including several dozen attempts to withdraw money out of his bank account, an attempt by an unauthorized actor to open an Apple credit card in his name in early 2024, and multiple unauthorized charges made on his credit and debit cards. As a result of this fraudulent conduct, Plaintiff Gill had to change multiple credit cards and multiple banks that he has used since the Data Breach.

22. Plaintiff Gill also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which occur daily, as well receiving notifications from Experian Identity Works on May 14, 2024, Feb 15, 2024, Jan 11, 2024, Jan 4, 2024, Dec 26, 2023, Dec 18, 2023, and Nov 22, 2023, that his PII was located on the dark web, which, upon information and belief, were caused by the Data Breach.

23. As a result of the Data Breach, Plaintiff Gill anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

24. Plaintiff **Carey Hylton** ("Plaintiff Hylton") is a citizen and resident of the state of California. Plaintiff Hylton has been a Caesars Reward member for at least 10 years. Plaintiff Hylton also currently holds a Caesars credit card, which she obtained in the summer of 2022. Plaintiff Hylton regularly gambled with Caesars both online and in person and has stayed at Caesars hotels at least twice a year for several years, at which time Caesars regularly collected her PII.

25. To obtain her membership, Plaintiff Hylton was required to provide Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Hylton was required to provide to obtain her Caesars Rewards membership.

26. On or around October 2023, Plaintiff Hylton learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including her name, driver's license number, social security number, and other data

contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

27. Plaintiff Hylton has been careful to protect and monitor her identity. Plaintiff Hylton had credit monitoring coverage before the Data Breach with LifeLock, which she obtained in 2021. In response to the Data Breach and threat to her PII, Plaintiff Hylton continued to pay for this service ($10/month for two more months), in addition to an attempt to purchase the credit monitoring service offered by Caesars (but was denied enrollment in such service).

28. As a result of the Data Breach, Plaintiff Hylton made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the increase in disruptive scam phone calls, texts, and emails she has received since the Data Breach. Plaintiff Hylton has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

29. Despite these efforts, Plaintiff Hylton suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (late fees she was required to pay for fraudulent Caesars credit card charges); (ii) damage and loss of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) nominal and statutory damages; and (x) the continued and certainly increased risk of identity theft and fraud.

30. In addition, as a result of the Data Breach, Plaintiff Hylton has experienced several fraudulent credit card charges on her Caesars' credit card, which resulted in her incurring late fees imposed on her by Caesars.

31. Plaintiff Hylton also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

32. As a result of the Data Breach, Plaintiff Hylton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

33. Plaintiff **Miguel Rodriguez** ("Plaintiff Rodriguez") is a citizen and resident of the state of California. Plaintiff Rodriguez regularly gambled with Caesars both online and in person, at which time Caesars regularly collected his PII.

34. To obtain his membership, Plaintiff Rodriguez was required to provide Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Rodriguez was required to provide to obtain his Caesars Rewards membership.

35. On or around September 2023, Plaintiff Rodriguez learned of the Data Breach from media coverage and has not, to date, received a notice letter from Caesars, notifying him of the specific PII of his that was accessed by dangerous criminals through the Data Breach. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

36. As a result of the Data Breach, Plaintiff Rodriguez made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to dealing with the numerous specific instances of identity theft and fraudulent activity that he experienced (as detailed below), monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

37. Despite these efforts, Plaintiff Rodriguez suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory

damages; and (xi) the continued and certainly increased risk of identity theft and fraud.

38. In addition, as a result of the Data Breach, Plaintiff Rodriguez has suffered actual injury in the form of experiencing numerous fraudulent attempts to open credit or bank accounts on his name, including US Bank notifying him that in October 2023 that someone had attempted to open a US Bank account in his name in Minnesota, which he did not authorize, resulting in Plaintiff Rodriguez needing to close his bank account. Plaintiff Rodriguez has also experienced several unauthorized inquiries that appeared on his credit report.

39. Plaintiff Rodriguez also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification on April 16, 2024, that his PII was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

40. As a result of the Data Breach, Plaintiff Rodriguez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

**2. Illinois Plaintiffs**

41. Plaintiff **April Elvidge** ("Plaintiff Elvidge") is a citizen and resident of the state of Illinois. Plaintiff Elvidge has been a Caesars Reward member since January 2021. Plaintiff Elvidge regularly gambled with Caesars both online and in person at which time Caesars regularly collected her PII.

42. To obtain her membership, Plaintiff Elvidge was required to provide Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Elvidge was required to provide to obtain her Caesars Rewards membership.

43. On or around October 2023, Plaintiff Elvidge learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including her name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was

subsequently revealed.

44. Plaintiff Elvidge has been careful to protect and monitor her identity. She had credit monitoring coverage through Capital One at the time that the Caesars' breach was announced.

45. As a result of the Data Breach, Plaintiff Elvidge made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the 10+ disruptive spam phone calls and 3+ spam texts that she receives on a daily basis. Plaintiff Elvidge has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

46. Despite these efforts, Plaintiff Elvidge suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (late fees she was required to pay for fraudulent Caesars' credit card charges); (ii) damage and loss of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) nominal and statutory damages; and (x) the continued and certainly increased risk of identity theft and fraud. Plaintiff Elvidge also suffered actual injury in the form of a significant increase in spam calls (about 10 per day) and spam texts (about 3 per day) and receiving a notification from a credit protection account she uses that her information was located on the dark web.

47. As a result of the Data Breach, Plaintiff Elvidge anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

48. Plaintiff **Charles Popp** ("Plaintiff Popp") is a citizen and resident of the state of Illinois. Plaintiff Popp has been a Caesars Reward member during the relevant time period. Plaintiff Popp regularly gambled with Caesars using its sportsbook app, at which time Caesars regularly collected his PII.

49. To obtain his membership, Plaintiff Popp was required to provide Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Popp was required to provide to obtain his Caesars Rewards membership.

50. On or around October 2023, Plaintiff Popp learned of the Data Breach from a letter sent to her by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including her name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

51. Plaintiff Popp has been careful to protect and monitor his identity. He had credit monitoring coverage at the time that the Data Breach was announced.

52. As a result of the Data Breach, Plaintiff Popp made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: changing email passwords several times, monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the increase in disruptive scam phone calls, texts, and emails he has received since the Data Breach. Plaintiff Popp has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

53. Despite these efforts, Plaintiff Popp suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud.

54. In addition, Plaintiff Popp suffered actual injury in the form of experiencing an

increase in spam calls, texts, and/or emails and receiving a notification from Credit Karma approximately six months ago that his PII was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

55. As a result of the Data Breach, Plaintiff Popp anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

56. Plaintiff **John Gedwill** ("Plaintiff Gedwill") is a citizen and resident of the state of Illinois. Plaintiff Gedwill has been a Caesars Reward member for at least two years. Plaintiff Gedwill regularly gambled with Caesars both online and in person at which time Caesars regularly collected his PII.

57. To obtain his membership, Plaintiff Gedwill was required to provide Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Gedwill was required to provide to obtain his Caesars Rewards membership.

58. On or around October 2023, Plaintiff Gedwill learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

59. Plaintiff Gedwill has been careful to protect and monitor his identity. He monitors his credit through Annual Credit Report.com.

60. As a result of the Data Breach, Plaintiff Gedwill made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to telephone conversations with his bank about the Data Breach and protecting his accounts from fraudulent use, monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received since the Data Breach.

61. Despite these efforts, Plaintiff Gedwill suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud.

62. In addition, as a result of the Data Breach, Plaintiff Gedwill has experienced a phishing attempt in which a stranger sent him money and requested that he return it.

63. Plaintiff Gedwill also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

64. As a result of the Data Breach, Plaintiff Gedwill anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

65. Plaintiff **Laura McNichols** ("Plaintiff L. McNichols") is a citizen and resident of the state of Illinois. Plaintiff L. McNichols has been a Caesars Reward member during the relevant time period. Plaintiff L. McNichols regularly gambled with Caesars both online and in person at which time Caesars regularly collected her PII.

66. On or around October 2023, Plaintiff L. McNichols learned of the Data Breach from a news article and has not, to date, received a notice letter from Caesars, notifying her of the specific PII of hers that was accessed by dangerous criminals through the Data Breach. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

67. To obtain her membership, Plaintiff L. McNichols was required to provide Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff L. McNichols was required to provide to obtain her Caesars

Rewards membership.

68. Plaintiff L. McNichols has been careful to protect and monitor her identity, including through the use of credit monitoring coverage through T-Mobile before the Data Breach.

69. As a result of the Data Breach, Plaintiff L. McNichols made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received since the Data Breach.

70. Despite these efforts, Plaintiff L. McNichols suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (late fees she was required to pay for fraudulent Caesars' credit card charges); (ii) damage and loss of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) nominal and statutory damages; and (x) the continued and certainly increased risk of identity theft and fraud. In addition, as a result of the Data Breach, Plaintiff L. McNichols has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification from T-Mobile that her Social Security numbers was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

71. As a result of the Data Breach, Plaintiff L. McNichols anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

72. Plaintiff **Thomas McNichols** ("Plaintiff T. McNichols") is a citizen and resident of the state of Illinois. Plaintiff T. McNichols has been a Caesars Reward member during the relevant time period. Plaintiff T. McNichols regularly gambled with Caesars both online and in person at which time Caesars regularly collected his PII.

73. On or around October 2023, Plaintiff T. McNichols learned of the Data Breach

from a news article and has not, to date, received a notice letter from Caesars, notifying him of the specific PII of his that was accessed by dangerous criminals through the Data Breach. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

74. To obtain his membership, Plaintiff T. McNichols was required to provide Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff T. McNichols was required to provide to obtain his Caesars Rewards membership.

75. Plaintiff T. McNichols has been careful to protect and monitor his identity, including through the use of credit monitoring coverage through T-Mobile before the Data Breach.

76. As a result of the Data Breach, Plaintiff T. McNichols made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

77. Despite these efforts, Plaintiff T. McNichols suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud. In addition, as a result of the Data Breach, Plaintiff T. McNichols has suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification from T-Mobile that his Social Security numbers was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

78. As a result of the Data Breach, Plaintiff T. McNichols anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused

by the Data Breach.

79. Plaintiff **Virginia Stacy** ("Plaintiff Stacy") is a citizen and resident of the state of Illinois. Plaintiff Stacy has been a Caesars Reward member during the relevant time period. Plaintiff Stacy regularly gambled with Caesars both online and in person, at which time Caesars regularly collected her PII.

80. On or around October 2023, Plaintiff Stacy learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including his name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

81. To obtain her membership, Plaintiff Stacy was required to provide Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Stacy was required to provide to obtain her Caesars Rewards membership.

82. Plaintiff Stacy has been careful to protect and monitor her identity, including through the use of credit monitoring coverage Credit Wise and Capital One.

83. As a result of the Data Breach, Plaintiff Stacy made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to taking actions to prevent numerous attempts of fraudulent activity that she experienced (as detailed below), freezing her credit, monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received since the Data Breach.

84. Despite these efforts, Plaintiff Stacy suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (late fees she was required to pay for fraudulent Caesars' credit card charges); (ii) damage and loss of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breach; (ix) nominal and statutory damages; and (x) the continued and certainly increased risk of identity theft and fraud. .

85. In addition, as a result of the Data Breach, Plaintiff Stacy has suffered actual injury in the form of an unauthorized actor opening a credit card in her name that was used to attempt to purchase a car and a Verizon phone.

86. As a result of the Data Breach, Plaintiff Stacy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

87. Plaintiff **Edward Cherveny** ("Plaintiff Cherveny") is a citizen and resident of the state of Illinois. Plaintiff Cherveny has been a Caesars Reward member during the relevant time period. Plaintiff Cherveny regularly gambled with Caesars in person at which time Caesars regularly collected his PII.

88. To obtain his membership, Plaintiff Cherveny was required to provide Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Cherveny was required to provide to obtain his Caesars Rewards membership.

89. On or around October 2023, Plaintiff Cherveny learned of the Data Breach from an email communication sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

90. As a result of the Data Breach, Plaintiff Cherveny made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

91. Despite these efforts, Plaintiff Cherveny suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs

(ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud. Plaintiff Cherveny also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails since the Data Breach, which, upon information and belief, was caused by the Data Breach.

92. As a result of the Data Breach, Plaintiff Cherveny anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

**3. Minnesota Plaintiffs**

93. Plaintiff **Cynthia Rubner** ("Plaintiff C. Rubner") is a citizen and resident of the state of Minnesota. Plaintiff C. Rubner has been a Caesars Reward member during the relevant time period. Plaintiff C. Rubner regularly stayed at Caesars' resorts, at which time Caesars regularly collected her PII.

94. To obtain her membership, Plaintiff C. Rubner was required to provide Caesars with her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff C. Rubner was required to provide to obtain her Caesars Rewards membership.

95. On or around October 2023, Plaintiff C. Rubner learned of the Data Breach from a letter sent to her by Caesars, notifying her that Caesars had allowed dangerous criminals to access her PII including her name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

96. As a result of the Data Breach, Plaintiff C. Rubner made reasonable efforts to

mitigate the impact of the Data Breach, including but not limited to contacting Caesars' customer service in an attempt to learn more about the Data Brach, calling her bank to inform it of the breach, and checking bank statements for herself and her husband about three times daily.

97. Despite these efforts, Plaintiff C. Rubner suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (late fees she was required to pay for fraudulent Caesars' credit card charges); (ii) damage and loss of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) nominal and statutory damages; and (x) the continued and certainly increased risk of identity theft and fraud. In addition, Plaintiff C. Rubner has also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

98. As a result of the Data Breach, Plaintiff C. Rubner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

99. Plaintiff **William Rubner** ("Plaintiff W. Rubner") is a citizen and resident of the state of Minnesota. Plaintiff W. Rubner has been a Caesars Reward member for at least four years. Plaintiff W. Rubner regularly stayed at Caesars resorts, at which time Caesars regularly collected his PII.

100. To obtain his membership, Plaintiff W. Rubner was required to provide Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff William Rubner was required to provide to obtain his Caesars Rewards membership.

101. On or around October 2023, Plaintiff W. Rubner learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access her PII including his name, driver's license number, social security number, and other data

contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

102. Plaintiff W. Rubner has been careful to protect and monitor his identity, including through the use of credit monitoring coverage LifeLock.

103. As a result of the Data Breach, Plaintiff W. Rubner made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received since the Data Breach.

104. Despite these efforts, Plaintiff W. Rubner suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud. Plaintiff W. Rubner also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails and receiving a notification from LifeLock since the Data Breach that his PII was discovered on the dark web, which, upon information and belief, was caused by the Data Breach.

105. As a result of the Data Breach, Plaintiff W. Rubner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

**4. New York Plaintiffs**

106. Plaintiff **Crystal Brewster** ("Plaintiff Brewster") is a citizen and resident of the state of New York. Plaintiff Brewster has been a Caesars Reward member for at least ten years. Plaintiff Brewster regularly gambled with Caesars both online and in person, at which time Caesars regularly collected her PII.

107. To obtain her membership, Plaintiff Brewster was required to provide Caesars with

her PII, including her name, address, driver's license number, email address, phone number, Social Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Brewster was required to provide to obtain his Caesars Rewards membership.

108. On or around October 2023, Plaintiff Brewster learned of the Data Breach from a letter sent to her by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including her name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

109. Plaintiff Brewster has been careful to protect and monitor her identity. She paid $24.99/month for credit monitoring coverage at the time of the Data Breach.

110. As a result of the Data Breach, Plaintiff Brewster made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: changing her telephone number, monitoring her credit card and checking account statements for any signs of fraudulent activity, monitoring her credit report, and managing the disruptive scam phone calls, texts, and emails she has received 3-5 times every day since the Data Breach. Plaintiff Brewster has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

111. As a result of the Data Breach, Plaintiff Brewster made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to attempting to contact Caesars at the beginning of the breach. She has also spent time reviewing account statements closely, logging into online accounts to check activity, signing up for credit monitoring, obtaining credit freezes, obtaining credit reports, researching news coverage about the breach, reading breach news almost daily. She visited her bank (over 1,000 miles over 9 months) and reset her billing.

112. Despite these efforts, Plaintiff Brewster suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (late fees she was required to pay for fraudulent Caesars' credit card charges); (ii) damage and loss

of the value of her PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of her PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) nominal and statutory damages; and (x) the continued and certainly increased risk of identity theft and fraud. In addition, since the Data Breach, Plaintiff Brewster has experienced constant and repeated attempts of identity theft and fraud which did not occur before the Data Breach, including: (i) a Fortiva credit card being opened in her name of which she had no knowledge; (ii) multiple inquiries made in her name to open automobile loans that she knew nothing about; (iii) an authorized charge appearing on her Bank of America account which she was forced to dispute; (iv) receiving a notice attempting to illicit payment from her based on claims that she was past due on payments owed to Verizon Wireless, despite her not having a Verizon account; (v) being compelled to close multiple bank accounts with Bank of America and Merryl Lynch due to frequent unauthorized charges being made; (vi) being compelled to change her telephone number due to the frequency of spam communications she has received since the Data Breach; and (vii) changing her name due to the above attempted acts of identity theft and fraud that have taken place since the Data Breach.

113. Plaintiff Brewster also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

114. As a result of the Data Breach, Plaintiff Brewster anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

115. Plaintiff **Isaac Dwek** ("Plaintiff Dwek") is a citizen and resident of the state of New York. Plaintiff Dwek has been a Caesars Reward member during the relevant time period. Plaintiff Dwek regularly gambled with Caesars both online and in person, at which time Caesars regularly collected his PII.

116. To obtain his membership, Plaintiff Dwek was required to provide Caesars with his PII, including his name, address, driver's license number, email address, phone number, Social

Security number, and date of birth. Upon information and belief, Caesars received and maintains the information Plaintiff Dwek was required to provide to obtain his Caesars Rewards membership.

117. On or around October 2023, Plaintiff Dwek learned of the Data Breach from a letter sent to him by Caesars, notifying him that Caesars had allowed dangerous criminals to access his PII including his name, driver's license number, social security number, and other data contained in Caesars' database. Coforge's conduct along with Caesars' for the Data Breach was subsequently revealed.

118. Plaintiff Dwek has been careful to protect and monitor his identity. At the time of the Data Breach, Plaintiff Dwek used a Credit Karma credit monitoring service. Plaintiff Dwek had used this service since about 2014.

119. As a result of the Data Breach, Plaintiff Dwek made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: monitoring his credit card and checking account statements for any signs of fraudulent activity, monitoring his credit report, and managing the disruptive scam phone calls, texts, and emails he has received 3-5 times every day since the Data Breach. Plaintiff Dwek has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

120. Despite these efforts, Plaintiff Dwek suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) out-of-pocket costs (ex. credit monitoring service); (ii) damage and loss of the value of his PII; (iii) loss of time; (iv) invasion of privacy; (v) theft of his PII; (vi) lost value of PII; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (ix) daily fear and anxiety about what he may face next; (x) nominal and statutory damages; and (xi) the continued and certainly increased risk of identity theft and fraud. In addition, Plaintiff Dwek has also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

121. As a result of the Data Breach, Plaintiff Dwek anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

**B. Defendants**

122. Defendant Coforge, Inc. (formerly NIIT Technologies Inc.) is a subsidiary of Coforge, Ltd. and a corporation organized under the laws of the state of Georgia, with its principal offices located in Princeton, New Jersey. Coforge is registered with the Secretary of State in California, Illinois, and Nevada, and conducts business within those states.

123. Defendant Coforge, Ltd. (formerly NIIT Technologies Ltd.) is a publicly traded company incorporated in the Republic of India, with its principal executive offices and registered office located in New Delhi, India. Defendant operates its business through subsidiaries of Coforge, Ltd., including Coforge, Inc., which directed business activities toward Nevada.

## III. JURISDICTION AND VENUE

124. This Court has subject matter jurisdiction over the action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs, there are more than 100 Class Members, and several Plaintiffs and at least one Class Member is a citizen of a state different than Defendant.

125. This Court has personal jurisdiction over Coforge because it is authorized to and regularly conducts business in Nevada and has sufficient minimum contacts in Nevada such that Coforge intentionally avails itself of this Court's jurisdiction by conducting operations here and promoting, selling, and marketing its services in this District. Coforge contracted to provide certain data security services for Caesars in Las Vegas, Nevada, which covered Plaintiffs' and Class Members' PII and, in exchange, agreed to be sued in and bound by any judgment rendered by a court in the state of Nevada concerning any disputes related thereto or interpretation of contracts related to services rendered for Caesars.

126. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Coforge conducts business in this District, and provided and continues to provide services to Caesars in this District

by stationing Coforge employees at a Las Vegas service desk.

## IV. STATEMENT OF FACTS

### A. Coforge's Business and its SOW with Caesars

127. Coforge, formerly NIIT Technologies, is an IT services and solutions firm. It offers "product engineering services, data services, cloud and infrastructure management services, digital process automation services and digital integration services" to industry.[10] Coforge represents over 260 clients worldwide, operates in 23 countries, and employs over 32,000 individuals. It reported $1 billion in revenue in 2023.

128. Coforge regularly partners with the hotel and casino industry. It represents on its website that it has been "a pioneering force in delivering cutting-edge solutions to the hospitality industry for over a decade" and has "managed IT solutions for over 60 hotels and casino properties globally," including for Caesars.[11] Coforge also touts its expertise in the hospitality industry in public SEC filings.[12]

129. Coforge contracted with Caesars to provide IT service desk operations since late 2012.[13] Coforge also provided "infrastructure change management, management of remote devices (including software management and distribution), and a device deployment core team."[14] Coforge was also tasked with "building a private cloud for a critical Help Desk application."[15]

130. Pursuant to the SOW, Coforge was to provide service desk services for both customers and Caesar employees to improve: (a) IT customer service and incident resolution speed through self-service abilities and skilled service desk staff in the areas of industry-standard IT

---

[10] Coforge, Who We Are, https://www.coforge.com/who-we-are (as of December 23, 2024); Coforge, Form F-1, Prospectus Summary Overview (July 20, 2022).

[11] Coforge, *Redefining Next Gen Experiences*, https://www.coforge.com/what-we-do/industries/travel-transportation-hospitality/hospitality/hotels-casinos-cruiselines (as of December 23, 2024).

[12] *See e.g.*, Coforge, Form F-1, *supra* n.11.

[13] Dr. Thomas Mendel, *Leapfrogging the Maturity S-Curve, How Caesars Entertainment and NIIT Technologies Moved Service Management to the Next Level of Maturity*, Hfs Research (July 10, 2013), https://www.hfsresearch.com/research/leapfrogging-maturity-s-curve/.

[14] *Id.*

[15] *Id.*

products and (b) Caesars efficiency and effectiveness by adopting best practices in the areas of custom reporting, logging, tracking, resolving IT incidents, and service requests. Coforge agreed to offer a friendly, customer service focused approach to all Caesars employees calling the service desk, and Coforge's personnel may have proved to be overly friendly to a fault.

131. Specifically, Coforge managed access to Plaintiffs' and Class Members' PII.

132. The SOW required Coforge to have its skilled staff take calls and approve or deny Caesars' employees' requests to re-set account passwords and to manage Caesars' security systems, including using multi-factor authentication because these systems could eventually access to Plaintiffs' and Class Members' PII. Coforge was required to have its personnel station the service desk in Las Vegas and an alternate location.

133. Coforge was also required to track and monitor calls to improve solutions and reduce wait times, accessing Caesars' monitoring tools as needed to troubleshoot incidents with Caesars' knowledge databases and vendor databases.

134. The SOW explicitly required Coforge to comply with a robust set of information security obligations to protect the PII that was exposed in the Data Breach. These obligations included: (a) administrative, technical, and physical safeguards to protect against accidental or unlawful destruction, alteration, unauthorized or improper disclosure or access to PII; (b) secure user identification and authentication protocols, including, when having access to Caesars' data systems and network: (c) appropriate background investigation of and enforceable confidentiality agreements with Coforge employees that would service Caesars; (d) individual privacy and security training and monitoring for Coforge employee compliance with the security program requirements; (e) restricting transmission of sensitive personal information to an encrypted format; (f) promptly and thoroughly investigation of all allegations, suspicions, and discoveries of unauthorized or improper access to, use, or disclosure of PII in Caesar's possession, and to immediately notify Caesars if it discovered unauthorized access; (g) bear all direct costs associated with resolving a security breach; and (h) carry appropriate insurance to address cybersecurity risks. The SOW further required Coforge to continually review and update it security compliance so that it is no less rigorous than industry practices, and to ensure a level of security appropriate to the

risks represented by the processing and the nature of Caesars' data.

135. Further, Coforge agreed to implement and maintain the following security frameworks and/or standards unless otherwise approved by Caesars in writing: (i) the OWASP Application Security Verification Standard (version 3.0 or newer), and (ii) either (A) the NIST Cyber Security Framework (version 1.1 or newer) or (B) the ISO/IEC 27001:2013 Information Security Management Systems standard (or any successor version).

136. Coforge agreed to take on a number of responsibilities to protect Caesars' data, including Plaintiffs' and Class Members' PII, including: implementing and maintaining an enterprise-wide risk management program; implementing and maintaining data security policies and standards; a single-sign on authentication service to access Coforge's system; and protecting Caesars' systems against and limiting the effects of attacks by unauthorized users.

137. Coforge was also required to use tools to monitor and audit events to aid in identification and logging of unauthorized use of its system or unauthorized access to Caesars' data, Plaintiffs' and Class Members' PII; review access to the system; and use the least privilege principle to limit access by users for the performance of specified tasks.

138. Coforge also agreed to abide by specified security incident procedures.

**B. Caesars' Business**

139. Caesars, formally known as Eldorado Resorts, operates more than 50 casino gaming and resort properties throughout the United States.

140. Caesars' loyalty program, Caesars Rewards, allows members to earn credits by betting on casino games, races, and sports games, both online and at Caesars' various properties, including on the Las Vegas Strip, and redeem them for more gaming or for hotel reservations, dining, shopping, and/or spa services.[16]

141. Plaintiffs and Class Members are current and former Caesars Rewards members.

142. As a condition of receiving its products and/or services, Caesars requires that its Caesars Rewards members, including Plaintiffs and Class Members, entrust it with highly sensitive

[16] Caesars Entertainment, Who We Are, https://www.caesars.com/corporate (as of July 19, 2024).

personal information such as their full legal name, full address, date of birth, drivers' license number, and Social Security number.

143. The information held by Caesars in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

**C. The Data Breach**

144. On August 18, 2023, a hacking group, known as Scattered Spider (or UNC3944), gained access to the Caesars Rewards member database through a social engineering attack on Coforge and downloaded the unencrypted PII of a significant number of Caesars Rewards 56 million members on or around August 23, 2023.[17] Scattered Spider is known for using social engineering to trick employees of the target company into granting them access to their network.[18] Scattered Spider threat actors monetize access to victim networks in numerous ways including extortion-enabled ransomware and data theft.[19] Thus, they may double-dip: force the target to pay to decrypt their data, while they also sell the exfiltrated data.

145. Scattered Spider gained access to Caesars' inadequately secured data IT network through a social engineering attack on Coforge. Upon information and belief, Coforge allowed the attackers to gain access to Caesars' network by resetting password(s) and bypassing multi-factor authentication settings for Caesars' network accounts without obtaining proper authentication.

146. As reported, Caesars offered to pay $15 million, about half the ransom demand, to Scattered Spider as ransom following the Data Breach.[20]

147. On September 7, 2023, Caesars' internal investigation confirmed that Scattered

[17] Office of the Maine Attorney General Data Breach Notification, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b21dc5d1-0bee-4a4c-92dc-bef4bbb519c9.shtml (as of July 19, 2024); Whittaker, *supra* n. 5.

[18] Whittaker, *supra* n. 5.

[19] Cybersecurity & Infrastructure Security Agency, Cybersecurity Advisory, "Scattered Spider," (AA23-320A) (Nov. 16, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a.

[20] Thomas Barrabi, *Caesar's Entertainment paid about $15m to hackers who stole customer Social Security numbers, other info: report*, N.Y. Post (Sept. 14, 2023, 2:24 PM), https://nypost.com/2023/09/14/caesars-entertainment-paid-about-15m-to-hackers-who-stole-customer-social-security-numbers-other-info-report/.

Spider had acquired, among other data, a copy of its loyalty program database including: names, driver's license numbers, and Social Security numbers for a significant number of Caesars Rewards' tens of millions of members.[21]

148. Caesars has not, to this date, publicly disclosed: how many of its loyalty rewards program members were affected by the Data Breach; what information was taken; how the cybercriminals were able to exploit vulnerabilities in Caesars' data systems; the identity of the hacking group responsible for the Data Breach; or what steps Caesars has taken to ensure that such an attack does not happen again.

149. Although Caesars still has not disclosed the precise nature and scope of the data exfiltrated in the Data Breach, upon information and belief, the data likely consists of tens of millions of customers' PII including names, addresses, phone numbers, and dates of birth, as well as driver's license numbers, and Social Security numbers.[22]

150. As a billion-dollar publicly traded company, Coforge had the financial wherewithal and personnel necessary to prevent the Data Breach. Yet, Coforge failed to adopt or comply with adequate IT security measures.

**D. Coforge Knew or Should Have Known Caesars Was a Likely Target of Cybercriminals**

151. Caesars operates both hotels and casinos. The type of PII collected by the hospitality and accommodation industry is particularly appealing to cybercriminals.

152. Trustwave's "2018 Global Security Report" listed hospitality as one of the top three industries most vulnerable to payment card breaches.[23] Other estimates project that hotels are the

[21] Ken Ritter, *Casino giant Caesars Entertainment hit by cyberattack, joining rival MGM Resorts as victim of data breach*, Fortune (Sept. 14, 4:02 AM), https://fortune.com/2023/09/15/caesars-entertainment-cyberattack-mgm-resorts-data-breach/.

[22] Zeba Siddiqui, *Hackers say they stole 6 terabytes of data from casino giants MGM, Caesars*, Reuters (Sept. 14, 2023, 3:16 PM), https://www.reuters.com/business/casino-giant-Caesars-confirms-data-breach-2023-09-14/.

[23] *See* Lena Combs & Joshua Davis, *Why Cybersecurity Matters*, Hotel Management (Oct. 17, 2019, 10:40 AM), https://www.hotelmanagement.net/tech/why-cybersecurity-matters.

targets of around 20% of all cyberattacks.[24]

153. In its 2018 Data Breach Investigations Report, Verizon noted that 15% of all data breaches occurring in 2017 involved the accommodation and food services industry.[25] The report noted that there were 338 breaches in the accommodation industry in 2017 alone, including at many of the major hotel brands.[26]

154. In recent years, Choice Hotels, Hard Rock Hotel, Hilton, Hyatt, Kimpton, Marriott, Millennium, Omni, Radisson, Starwood, and Wyndham, among others, have all experienced data breach incidents.[27]

155. "Such unfortunate trends should not come as much of a surprise since hotels are hotbeds of sensitive information. Their data is spread out across porous digital systems…."[28]

156. While hospitality companies have fewer transactions than retail organizations, they collect substantially more valuable and varied personal data for each of their guests. This rich personal data is invaluable to cybercriminals. They can use this data to better impersonate each breached customer, leading to additional identity theft and social engineering attacks. By enabling further attacks, breaching a hotel provides cybercriminals much more value than breaching a company in almost any other industry.[29]

157. But even if none of this alerted Coforge as to the foreseeability of a cyberattack on Caesars' data, the contract with Caesars must have because it conveyed to Coforge ***at least*** the

---

[24] *Id.*

[25] *See Verizon 2018 Data Breach Investigations Report*, 11th Ed., at pp. 5, 25, 27, *available at* https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

[26] *Id.*

[27] *See Timeline: The Growing Number of Hotel Data Breaches*, CoStar.com (April 7, 2020, 10:50 AM), *available at* https://www.costar.com/article/139958097.

[28] *See* Combs, *supra* n. 23.

[29] Nirmal Kumar, *Cybersecurity in Hospitality: An Unsolvable Problem?*, HospitalityBiz (June 27, 2018) (now removed), https://web.archive.org/web/20211017182154/http:/www.hospitalitybizindia.com/detailNews.aspx?aid=28970&sid=42; *The challenges of hospitality cybersecurity: An unsolved problem?*, Deccan Chronicle (Aug. 23, 2018), https://www.deccanchronicle.com/technology/in-other-news/230818/the-challenges-of-hospitality-cybersecurity-an-unsolved-problem.html; *Cybersecurity in hospitality—a growing issue?*, CyberSmart (Mar. 23, 2021), https://cybersmart.com/2021/03/cybersecurity-in-hospitality-a-growing-issue/.

following: (a) Coforge would be managing access to Sensitive Personal Information including government issued identification numbers; (b) Coforge must hire personnel of integrity, who passed background checks, and who were properly trained in managing access to such information; and (c) a security breach was foreseeable, requiring Coforge to limit access to its system, monitor unauthorized access, investigate security incidents, and possibly pay for notification and remediation if Coforge failed in its obligations.

158. Coforge had obligations created by the FTC Act, state law, contract, industry standards, to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

159. The high risk of data breaches in the hospitality and gaming industries were widely known throughout the field, including to Coforge. [30]

160. Indeed, Coforge identified in its July 20, 2022 Form F-1 that cyberattacks were a significant risk factor faced by its clients, noting "Companies are also increasingly sensitive to data privacy and cybersecurity issues" and "negative experiences associated with offshore outsourcing, such as theft and misappropriation of sensitive client data" could materially and adversely impact its business."[31]

161. Thus, Coforge was aware of the high risk of data intrusions and the magnitude of the harm that could result from a breach.

[30] *Cybercrime Causing Insurance Issues for Casinos* (Jul. 4, 2022), https://www.casinos.us/news/casino-operators-experience-insurance-issues-due-to-cybercrime/; *Casinos must focus on cybersecurity for no deposit bonus codes*, Grande Vegas Casino, https://www.grandevegascasino.com/articles/casinos-must-focus-on-cybersecurity-for-no-deposit-bonus-codes (last visited Apr. 7, 2025); *FBI targets casino cybercrime*, Cyber Intelligence (Nov. 10, 2023), https://cyberintel.media/fbi-targets-casino-cybercrime/; Private Industry Notification, FBI (Nov. 7, 2023), https://www.aha.org/system/files/media/file/2023/11/bi-tlp-clear-pin-ransomware-actors-continue-to-gain-access-through-third-parties-and-legitimate-system-tools-11-7-23.pdf; Noa Bar-Yosef, *Hacking the House: How Cybercriminals Attack Online Casinos*, SecurityWeek (Aug. 2, 2011), https://www.securityweek.com/hacking-house-how-cybercriminals-attack-online-casinos/.

[31] Coforge, Form F-1, *supra* n.11.

**E. Coforge Failed to Comply with Established Cybersecurity Frameworks and Industry Standards.**

162. Coforge implemented knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, despite claiming to use "state-of-the-art technologies"[32] and "strict access controls and user authentication measures."[33]

163. The FTC has promulgated various guides for businesses, which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[34]

164. In 2016, the FTC updated its publication titled *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[35] The guidelines noted that businesses should warn employees about phone phishing, and in particular callers asking for employee contact information.

165. In another publication, the FTC recommends that companies require complex passwords to be used on networks; require robust use of multi-factor authentication; protect against authentication bypass; use industry-tested methods for security; and monitor for suspicious activity on the network.[36]

166. The FTC has brought several enforcement actions against businesses for failing to adequately protect customer data.

167. Importantly for current purposes, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the Federal Trade

---

[32] Coforge, Meet Global Data Protection Standards with Coforge-s Data Security Solutions, *supra* n.12.

[33] *Id.*

[34] *See Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited July 26, 2024).

[35] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct. 2016, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited July 26, 2024).

[36] *See Start With Security: A Guide for Business*, *supra* n. 34.

Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

168. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

169. In its 2019 Privacy & Data Security Update, the FTC noted that "[s]ince 2002, the FTC has brought more than 70 cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data."[37]

170. In this case, Coforge was fully aware from its contract with Caesars and its industry experience of its obligation to use reasonable and adequate measures to protect consumers' PII. Coforge also knew that the Caesars' network that it protected was a ripe target for hackers. Despite understanding the risks and consequences of inadequate data security, Coforge failed to comply with FTC data security obligations.

171. Coforge's failure to adopt or comply with reasonable safeguards to protect PII constitutes an unfair act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45.

172. Similarly, the National Institute of Standards and Technology (NIST) provides basic network security guidance enumerating steps to take to avoid cybersecurity vulnerabilities.[38] The NIST guidelines provide valuable insights and best practices to protect network systems and customer data, and these guidelines were addressed in Coforge's contract with Caesars.

173. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[39]

---

[37] *See Privacy & Data Security Update: 2019*, Federal Trade Commission, 2020, *available at* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf (last visited July 26, 2024).

[38] *See Framework for Improving Critical Infrastructure Cybersecurity*, Nat'l Inst. of Standards and Tech. (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. A new framework was published in 2024, after the Data Breach. *See* CSF 2.0 Resource Center, *available at* https://www.nist.gov/cyberframework (last accessed July 28, 2024).

[39] *Id*. at Table 2 pg. 26-43.

174. Further, cyber security experts have promulgated a series of best practices that should be implemented by hotels, including protecting web browsers and email management systems and training hotel staff regarding critical points.[40]

175. Shortly after the Data Breach, the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory (CSA) in response to Scattered Spider actions.[41] The CSA detailed Scattered Spider's social engineering techniques including "phishing, push bombing, and subscriber identity module (SIM) swap attacks, to obtain credentials, install remote access tools, and/or bypass multi-factor authentication (MFA)" and provided specific mitigation techniques to protect against them.[42] Upon information and belief, Scattered Spider used vishing to access and download the Caesars' Rewards database.

176. To mitigate against Scattered Spider's social engineering techniques, CISA and the FBI recommend:

> (a) Requiring authorized remote access solutions to be used only from within the network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
>
> (b) Implementing FIDO/WebAuthn authentication or Public Key Infrastructure (PKI)-based MFA. These MFA implementations are resistant to phishing and not susceptable to push bombing or SIM swap attacks, which are techniques known to be used by Scattered Spider actors.
>
> (c) Requiring phishing-resistant multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.[43]

177. Coforge was, or should have been, aware of and implemented these mitigation techniques prior to Data Breach as they were publicly available and appeared in CISA's publications such as its *Guide to Securing Remote Access Software*,[44] *Implementing Phishing-*

---

[40] *See How to Work on Hotel Cyber Security*, Open Data Security (July 23, 2019), *available at* https://opendatasecurity.io/how-to-work-on-hotel-cyber-security/.

[41] Cybersecurity Advisory Scattered Spider (AA23-320A), *supra* n. 20.

[42] *Id.*

[43] *Id.*

[44] CISA, Guide to Securing Remote Access Software (June 6, 2023),

*Resistant MFA*,[45] and *Cross-Sector Cybersecurity Performance Goals*.[46] Indeed, Coforge's contract with Caesars required multifactor authentication, including when resetting passwords, to control access to Caesar's data, including Plaintiffs' and Class Members' PII. Upon information and belief, Coforge failed to adequately implement these techniques as evidenced by the Data Breach.

178. Coforge's failure to protect Plaintiffs and Class Members' PII illustrates Coforge's failure to adhere to the spirit and letter of the FTC guidelines, NIST guidance, and industry best practices.

**F. Plaintiffs and Class Members Suffered and Will Continue to Suffer Injuries**

179. Coforge's failure to keep the PII of Plaintiffs and Class Members secure has severe ramifications. Plaintiffs and Class Members face a high risk of misuse of their PII from the Data Breach. Upon information and belief, the hackers perpetrated a social engineering attack on Coforge and stole PII from Caesars with the specific intent to use it for illicit purposes and/or sell it to others to be misused. And the hackers have carried out this intent by using the data to demand a ransom payment from Caesars.

180. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Coforge to keep their PII confidential and securely maintained, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

**1. Actual and Attempted Fraud and Mitigation Efforts**

181. Plaintiffs' PII is now in the hands of Scattered Spider (and to those Scattered Spider

---

https://www.cisa.gov/sites/default/files/2023-06/Guide%20to%20Securing%20Remote%20Access%20Software_clean%20Final_508c.pdf.

[45] CISA, Implementing Phishing-Resistant MFA (Oct. 2022), https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

[46] CISA, Cross-Sector Cybersecurity Performance Goals, v1.01 (March 2023), https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

distributed it), described by Microsoft as "one of the most dangerous financial criminal groups."[47] Scattered Spider's criminal activity is so prolific that following the Data Breach, the FBI and CISA released published the CSA to "encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA *to reduce the likelihood and impact of a cyberattack by Scattered Spider actors*."[48]

182. As noted in Section, II.A., PII of the Plaintiffs and Class Members have already been misused and exploited for fraud. In addition, Scattered Spider is known to have exfiltrated data to "multiple sites included U.S.-based data centers and MEGA.NZ."[49]

183. Plaintiffs and Class Members have already incurred or will incur out of pocket costs as a result of the Data Breach. As an example, Plaintiff Gill has spent $400 for a one-year subscription for identify protection services.

184. Plaintiffs' PII has already been found on the dark web and Plaintiffs' experience measurable increases in targeted identity theft attempts.

185. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial and other accounts for fraud; researching and disputing suspicious or fraudulent activity; obtaining and reviewing credit reports; placing credit freezes on their credit profiles; dealing with spam and phishing emails, text messages, and phone calls; and reviewing their financial affairs more closely than they otherwise would have, among other things. These efforts are burdensome and time-consuming and would not have been necessary but for Coforge's data security shortfalls.

186. Even in instances where a Class Member is reimbursed for a financial loss due to fraud, that does not make the individual whole again because there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing

---

[47] *Microsoft Warns as Scattered Spider Expands from SIM Swaps to Ransomware*, The Hacker News (Oct. 26, 2023), https://thehackernews.com/2023/10/microsoft-warns-as-scattered-spider.html.

[48] Cybersecurity Advisory Scattered Spider (AA23-320A), *supra* n. 20.

[49] *Id.*

up the issues" relating to fraud and identity theft.[50]

**2. Loss of Value of PII**

187. Plaintiffs and Class Members have also suffered a "loss of value of PII."

188. A robust market exists for stolen PII, which is sold and distributed on the dark web and through illicit criminal networks at specific, identifiable prices. Cybercriminals routinely market stolen PII online, making the information widely available to criminals across the world.

189. For example, stolen driver's license numbers can be sold for between $10 and $35 each.[51]

190. Stolen PII is a valuable commodity to identity thieves. The purpose of stealing large blocks of PII is to use it for illicit purposes or to sell it and profit from other criminals who buy the data and misuse it.

191. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[52] The Information Commissioner's Office in the European Union, when investigating a hotel data breach at Marriott, noted that "[p]ersonal data has a real value so organi[z]ations have a legal duty to ensure its security."[53]

192. Nevada law, too, acknowledges that personal information has intrinsic monetary value. Specifically, Nev. Rev. Stat. § 597.810 provides for statutory damages of $750 for

---

[50] *See Victims of Identity Theft*, U.S. Dept. of Justice (Nov. 13, 2017), *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 29, 2024).

[51] *See* Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec, 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; *How Cybercriminals Make Money*, Keeper, https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html (last visited July 26, 2024).

[52] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice (Feb. 10, 2020), *available at* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited July 26, 2024).

[53] *See Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach*, ICO News (July 9, 2019), *available at* https://edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en (last visited July 29, 2024).

unauthorized commercial use of a person's name, voice photograph, or likeness by companies conducting business in Nevada.

193. The value of personal information is increasingly evident in our digital economy. Many companies collect personal information for purposes of data analytics and marketing.

194. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[54]

195. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not from a price at which consumers themselves seek to sell it, but rather from the economic benefit consumers derive from being able to use it. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII leads to a loss of the value of the PII.

196. Beyond the immediate risk of actual harm, consumer victims of data breaches also lose the ability to negotiate sharing their PII for services, as their PII has value, and they have been deprived of that negotiated value because it was shared with an unauthorized third party without their consent. As a result, their PII may be used in the future (and, for several Plaintiffs, already has been used) for unauthorized purposes because of this Data Breach.[55]

**3. Criminals Will Continue to Use Class Members' Stolen PII for Years**

197. The risk of fraud following a data breach like this one persists for years. Identity

[54] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

[55] *See, e.g.,* James K. Wilcox, *Internet Providers Funded Campaign Yielding Millions of Fake Net Neutrality Comments, New York State Says*, Consumer Reports (May 6, 2021), https://www.consumerreports.org/electronics/net-neutrality/internet-providers-campaign-fake-net-neutrality-comments (noting how "lead generators" used information stolen from data breaches to create comments purportedly from those individuals victimized in the data breach supporting the termination of net neutrality, without obtaining consent or approval to make those comments).

thieves often hold stolen data for months or years before using it, to avoid detection and maximize profits. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because data is often broken into smaller batches when sold or re-sold to appeal to different types of buyers. In addition, stolen data may be distributed through off-line criminal networks and syndicated to be used for crime near where the victim resides.

198. According to a Government Accountability Office Report, the threat of future identity theft lingers for a substantial period of time after a data breach given the time lag between when information is stolen and when it is used:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[56]

199. Another source, discussing a similar data breach of Caesars' competitor MGM Resorts International, stated: "[A]s with many breaches, malicious actors sometimes wait months or years to tip their hand. . . . This is a great example of how these breaches and their fallout can continue to haunt businesses for quite some time. . . . "[57]

200. Accordingly, Plaintiffs and Class Members may not see the full extent of identity theft or misuse of their personal information for years to come. They face an ongoing risk and must vigilantly monitor their financial and other accounts indefinitely.

201. Moreover, even after Plaintiffs and Class Members' PII is misused, it may take months or years for them to become aware of the misuse. This complicates the process of disputing and correcting the misuse of their data.

---

[56] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, United States Government Accountability Office (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited July 19, 2024).

[57] *See* Doug Olenick, *MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine (Feb. 20, 2020), *available at* https://www.scmagazine.com/news/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers (last visited July 29, 2024).

**4. PII Stolen in This Data Breach Can be Combined with Data Acquired Elsewhere to Commit Identity Theft**

202. Identity thieves can combine PII stolen in the Data Breach with information gathered from other sources such as public sources or even the consumer's social media accounts, to commit identity theft. Thieves can then use the combined data profile to commit fraud including, among other things, opening new financial accounts or taking out loans in the consumer's name, using the consumer's information to obtain government benefits, filing fraudulent tax returns using the consumer's information and retaining the resulting tax refunds, obtaining a driver's licenses in the consumer's name but with another person's photograph, and giving false information to police during an arrest.

203. A federal district court has explained the process as follows:

> The threat of identity theft is exacerbated by what hackers refer to as "fullz packages." A fullz package is a dossier that compiles information about a victim from a variety of legal and illegal sources. Hackers can take information obtained in one data breach and cross-reference it against information obtained in other hacks and data breaches. So, for example, if a hacker obtains a victim's . . . health information from UnityPoint, the hacker can combine it with the same victim's Social Security number and phone number from a different data breach. This allows the hacker to compile a full record of information about the individual, which the hacker then sells to others as a package.

*Fox v. Iowa Health Sys*., 399 F. Supp. 3d 780, 789 (W.D. Wis. 2019).

204. Thieves can also use PII from the Data Breach, alone or in combination with other information about the consumer, to send highly targeted spear-phishing emails to the consumer to obtain more sensitive information. Spear phishing involves sending emails that look legitimate and are accompanied by correct personal and other information about the individual. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Bank of America, Amazon, or even a government entity), the individual provides sensitive information requested in the email. This could include login credentials, account numbers, or various other types of information.

205. Identity thieves can also use PII from the Data Breach in a "SIM swapping" attack to take control of consumers' phone numbers, allowing them to bypass 2-factor authentication to access the consumer's most sensitive accounts. In other words, fraudsters can use breached PII to

convince the consumer's mobile phone carrier to port-over the person's mobile phone number to a phone that the hacker controls. A journalist discussing a similar Data Breach of Caesars' competitor MGM described this scheme as follows:

> Exposed phone numbers create an additional risk: SIM swapping. In these scams, criminals use the data they've gathered about a potential victim to convince wireless carriers to move a number to a different phone. The goal is to intercept two-factor authentication codes that are delivered by SMS.[58]

## V. CLASS ACTION ALLEGATIONS

206. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and (c)(4).

207. Plaintiffs bring this action on their own behalf, and on behalf of the following Class and Subclasses (referred to collectively as the "Coforge Classes"):

- **Nationwide Class:** All persons residing in the United States whose PII was accessed in the Data Breach.

208. The Nationwide Class asserts claims against Coforge for Negligence (Count I).

209. Under the Restatement (Second) of Conflict of Laws §§ 145, adopted by Nevada courts and which applies to the facts here, Nevada substantive law controls the common law tort claims of Plaintiffs, regardless of Plaintiffs' state of residency.

210. The Plaintiffs who are citizens from California, Illinois, Minnesota, and New York also bring this action on their own behalf, and on behalf of the following Subclasses:

- ***California Subclass****:* All residents of California whose PII was accessed in the Data Breach. The proposed representatives for the California Subclass are Plaintiffs Gill, Hylton, and Rodriguez.
- ***Illinois Subclass:*** All residents of Illinois whose PII was accessed in the Data Breach. The proposed representatives for the Illinois Subclass are Plaintiffs Elvidge, Popp, Gedwill, L. McNichols, T. McNichols, Stacy, and Cherveny.
- ***Minnesota Subclass:*** All residents of Minnesota whose PII was accessed in the Data Breach. The proposed representatives for the Minnesota Subclass are Plaintiffs C. Rubner and W. Rubner.
- ***New York Subclass*****:** All residents of New York whose PII was accessed in the Data Breach. The proposed representatives for the New York Subclass are Plaintiffs Brewster and Dwek.

[58] *See* Lee Matthews, *For Sale: Hacked Data On 142 Million MGM Hotel Guests*, Forbes (July 14, 2020), *available at* https://www.forbes.com/sites/leemathews/2020/07/14/mgm-142-million-guests-hacked/?sh=1ca9d7125294 (last visited July 19, 2024).

211. The Subclasses assert statutory claims for violations of the Unfair Competition Law (UCL), Cal. Bus. & Prof. Code §§ 17200, *et seq.* (Claim for Relief II); Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, *et seq.* and 815 ILCS 530/45(a) (Claim for Relief III); Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.43, *et seq.* (Claim for Relief IV); and the New York General Business Law, N.Y. Gen. Bus. Law § 349 (Claim for Relief V).

212. Excluded from the Nationwide Class and Subclasses are Defendant's executive officers and directors, and the judges to whom this case is assigned, their immediate family members, and courtroom staff.

213. Plaintiffs reserve the right to amend the definitions of the Coforge Classes after having an opportunity to conduct discovery.

214. ***Numerosity: Fed. R. Civ. P. 23(a)(1).*** Upon information and belief, the Coforge Classes are so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, the class size can be determined by information available in Coforge's records, which will be a subject of discovery. On information and belief, there are millions of Class Members in the Coforge Classes.

215. ***Commonality: Fed. R. Civ. P. 23(a)(2).*** There are many "questions of law or fact" common to the Coforge Classes for purposes of Rule 23(a)(2), including but not limited to:

a. Whether Coforge's data security systems prior to the Data Breach complied with applicable data security laws, regulations, industry standards, and other relevant requirements;

b. Whether Coforge failed to take adequate and reasonable measures to ensure Caesars' data systems were protected;

c. Whether Coforge failed to take available steps to prevent and stop the breach from happening;

d. Whether Coforge owed a duty to Plaintiffs and Class Members to safeguard their PII;

e. Whether Coforge breached its duty to Plaintiffs and Class Members to safeguard their PII;

f. Whether Coforge's conduct, including its failure to act, resulted in or was the proximate cause of the breach of Caesars' systems, resulting in the unauthorized

access to and/or theft of its customers' PII;

g. Whether, as a result of Coforge's conduct, Plaintiffs and Class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

h. Whether, as a result of Coforge's conduct, Plaintiffs and Class members are entitled to equitable, declaratory, and/or other relief ,and, if so, the nature of such relief.

216. ***Typicality: Fed. R. Civ. P. 23(a)(3).*** Typicality is satisfied because the claims of Plaintiffs and all Class Members derive from the same operative facts. Plaintiffs and Class Members all had their PII stolen in the Data Breach. Plaintiffs and Class Members have the same basic legal claims against Coforge.

217. ***Adequacy of Representation: Fed R. Civ. P. 23(a)(4).*** Plaintiffs will fairly and adequately protect the interests of the Coforge Classes. Plaintiffs have retained competent counsel who are highly experienced in data breach class actions and other complex litigation. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Coforge Classes. Plaintiffs' counsel have the financial and personnel resources to litigate this matter through all phases of pretrial litigation, trial, and any necessary appeals. Neither Plaintiffs nor their counsel have any interests that are contrary to, or conflict with, those of the Coforge Classes.

218. ***Predominance: Fed. R. Civ. P. 23(b)(3).*** Coforge has engaged in a common course of conduct toward all Class Members. The common issues identified above arising from Coforge's conduct predominate over any issues affecting only individual Class Members. The common issues hinge upon Coforge's conduct rather than that of any individual plaintiff or class member. Adjudication of the common issues in a single action has important and desirable advantages that will lead to judicial economy.

219. ***Superiority: Fed. R. Civ. P. 23(b)(3).*** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law of fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of litigating their individual claims is prohibitively high and they would therefore have no realistic means to a remedy on an individual non-class basis. The litigation of separate actions by consumers would create a risk of inconsistent

or varying adjudications, which could establish incompatible standards of conduct for Coforge. In contrast, conducting this action on a class-wide basis presents fewer management difficulties, conserves judicial and party resources, and pursues the rights of all Class Members in a single proceeding.

220. ***Declaratory and Injunctive Relief: Fed. R. Civ. P. 23(c)(4).*** Coforge has acted or refused to act on grounds that apply generally to the Coforge Classes, so that final injunctive relief or corresponding declaratory relief is appropriate respecting those classes as a whole.

221. ***Certification of Issues: Fed. R. Civ. P. 23(c)(4).*** In the alternative, Plaintiffs request that the Court certify the case to proceed as a class action on particular issues, particularly liability as described herein, which would substantially advance the litigation to trial.

## VI. CAUSES OF ACTION

### CLAIM FOR RELIEF I

### NEGLIGENCE

***(Brought by all Plaintiffs on behalf of the Nationwide Class)***

222. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 221 as if fully set forth herein.

223. Coforge had knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could face if their PII was stolen in a data breach.

224. Coforge had a duty to exercise reasonable care in safeguarding, securing, and protecting Class Members' PII. This duty included, among other things, maintaining data security measures consistent with industry standards.

225. Coforge had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of Coforge's inadequate security practices. Coforge knew that its failure to detect and identify IT security threats could result in the exposure of Plaintiffs' and Class Members' Personal Information and cause significant harm, which Coforge acknowledged in its own public filings.

226. Coforge's duty to use reasonable data security measures also arose under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce,"

including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as Coforge. Various FTC publications and data security breach orders further form the basis of Coforge's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

227. Coforge also had a duty to safeguard the Personal Information of Plaintiffs and class members because of state laws and statutes that require Coforge to reasonably safeguard Personal Information, including but not limited to Nev. Rev. Stat. §603A.210, which states that businesses allowing for access to personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from authorized access."

228. Coforge was subject to an independent duty to the Plaintiffs and Class Members and no express contract between Coforge and Plaintiffs or Class Members exists. Sources of the independent duty are included in the list above, including the contract between Coforge and Caesars.

229. Coforge's violations of the FTC Act and state data security statutes constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs belong and to prevent the type of harm that resulted from the Data Breach.

230. Plaintiffs and Class Members were the foreseeable victims of Coforge's inadequate data security practices. Coforge knew that a breach of Caesars' systems could cause harm to Plaintiffs and Class Members.

231. Coforge's conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Coforge's misconduct included its failure to follow standard security practices to block unauthenticated access to Caesars' network, which held consumers' PII.

232. Coforge knew or should have known of the importance of providing adequate security, and the frequent cyberattacks aimed at the hospitality and gaming industry.

233. Plaintiffs and Class Members had no ability to protect their PII once it was in Caesars' possession and control. Coforge was in an exclusive position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

234. Coforge, through its actions and inactions, breached its duties owed to Plaintiffs and Class Members by failing to exercise reasonable care in safeguarding their PII.

235. Coforge inadequately safeguarded consumers' PII in deviation of standard industry rules, regulations, and best practices at the time of the Data Breach.

236. But for Coforge's breach of duties, consumers' PII would not have been stolen by a computer hacker.

237. Coforge's wrongful and negligent breach of its duties owed to Plaintiffs and class members caused their Personal Information to be compromised.

238. As a result of Coforge's conduct, Plaintiffs and Class Members suffered and will continue to suffer the various types of damages alleged herein—including, but not limited to, significant risk of substantial and immediate future harm, identity theft and fraud, additional time, resources, and money spent on mitigation efforts, increased phishing and attempts at fraud, and further loss of value of personal information.

239. Due to Defendant's conduct, Plaintiffs and Class Members are also entitled to identity protection and credit monitoring. Identity protection and credit monitoring are reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Plaintiffs and Class Members. There is no question that this PII was taken by sophisticated cybercriminals increasing the risks to the Plaintiffs and Class Members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring. Some experts recommend that data breach victims obtain credit monitoring services for many years after a data breach. Annual subscriptions for comprehensive credit monitoring plans that include inquiry alerts, credit locks, and identity theft insurance range from $219 to $329 per year.

240. Plaintiffs and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth above.

**CLAIM FOR RELIEF II**

**VIOLATION OF CAL. BUS. CODE § 17200 ("UCL"), *et seq.***

***(On behalf of California Plaintiffs and the California Subclass against all Defendants)***

241. The California Plaintiffs, individually and on behalf of the California Subclass, re-

allege and incorporate by reference Paragraphs 1 through 221 as if fully set forth herein.

242. California's Unfair Competition Law ("UCL") prohibits any person from committing an act of "unfair competition," including "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising . . . ." Cal. Bus. & Prof. Code § 17200.

243. "[U]nfair competition" is interpreted broadly to include acts that violate other laws and may include acts even if not specifically proscribed by some other law.

244. Coforge violated the UCL by engaging in conduct that constituted "unlawful . . . business practices," including by violating the FTC Act., and other state data security laws.

245. Specifically, Coforge failed to implement standard identity verification procedures before granting access to sensitive systems and failing to adequately train employees on how to detect and respond to common social engineering tactics such as vishing.

246. Specifically, Coforge managed access to Plaintiffs' and California Subclass's PII. Coforge implemented knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, despite claiming to use "state-of-the-art technologies" and "strict access controls and user authentication measures."

247. In the vishing attack, Coforge employees granted a password reset to a caller impersonating an internal Caesars employee without verifying the caller's identity. This enabled cybercriminals to gain unauthorized access to systems containing consumer PII.

248. Coforge's failure to implement basic industry-standard cybersecurity safeguards was also unfair and unlawful because it violated other California statutes. Specifically, Coforge violated the California Civil Code § 1798.150 by failing to employ reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or disclosure of California Plaintiffs' and the California Subclass's PII.

249. Coforge's failure to comply with basic data security necessary to protect stored PII constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to consumers. That is especially true because Coforge publicly claimed (and in its Agreement with

Caesars promised) to have robust security practices, while internally failing to implement even the most basic protections against foreseeable attack methods like vishing.

250. As a result of those unlawful and unfair business practices, California Plaintiffs and the California Subclass's highly sensitive and private PII was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the PII. Subsequently, the stolen information was posted on the dark web, exposing it and putting individuals at a substantial risk of misuse.

251. As a direct and proximate result of Coforge's inadequate security and the resulting Data Breach, California Plaintiffs and the California Subclass suffered and will continue to suffer significant injuries, including, but not limited to:

a. loss of privacy;

b. misappropriation of their identity, name and likeness;

c. fraud and identity theft from the misuse of their stolen PII;

d. diminution in the value of their PII due to the loss of security, confidentiality, and privacy;

e. lost value of their PII;

f. emotional and mental distress and anguish resulting from the access, theft and posting of their PII;

g. lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and

h. a continued substantial and imminent risk of the misuse of their PII.

252. California Plaintiffs and the California Subclass also remain at heightened risk of future injury because, based upon information and belief, Coforge continues to provide services to Caesars, and Coforge's inability to adopt or to comply with security standards to avoid unauthorized access to their PII puts them at continued risk. Without the use of adequate data security, they remain at a heightened and substantial risk that their PII will be subject to another data breach.

253. California Plaintiffs and the California Subclass seek all monetary and non-

monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and which the Court deems proper.

**CLAIM FOR RELIEF III**

**VIOLATION OF ILLINOIS CONSUMER FRAUD**

**AND DECEPTIVE BUSINESS PRACTICES ACT ("ICFA")**

**815 ILL. COMP. STAT. §§ 505, *et seq*.**

***(On behalf of Illinois Plaintiffs and the Illinois Subclass)***

254. Illinois Plaintiffs, individually and on behalf of the Illinois Subclass, re-allege and incorporate by reference Paragraphs 1 through 221 as if fully set forth herein.

255. The ICFA makes unlawful certain acts by persons in the conduct of trade or commerce. 815 Ill. Comp. Stat. § 505/2. Violating the Illinois Personal Information Protection Act ("IPIPA"), 815 Ill. Comp. Stat. 530/1, *et seq*., is one such unlawful act.

256. Coforge is a "data collector" as it is Caesars' third-party IT vendor that handles personal information of consumers while providing services for computerized data that includes personal information. IPIPA. 815 Ill. Comp. Stat. 530/5.

257. The IPIPA requires data collectors like Coforge that maintains "records that contain personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 Ill. Comp. Stat. § 530/45. Coforge, however, failed to implement and maintain reasonable security measures as required by the statute.

258. Specifically, Coforge managed access to Illinois Plaintiffs' and the Illinois Subclass's PII. Coforge failed to protect that data from a known and preventable threat — a social engineering attack known as vishing, in which cybercriminals impersonated employees over the phone to gain access credentials. Despite holding itself out as a cybersecurity expert, Coforge did not implement adequate training or safeguards to prevent its personnel from granting access based on a phone call without proper identity verification.

259. Specifically, Coforge failed to implement standard identity verification procedures before granting access to sensitive systems and failing to adequately train employees on how to detect and respond to common social engineering tactics such as vishing.

260. Coforge implemented knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, despite claiming to use "state-of-the-art technologies" and "strict access controls and user authentication measures," Coforge deployed unreasonably deficient security measures that defied expert recommendations, industry standards, and statutory requirements. Coforge did not have adequate verification protocols in place for password reset requests, nor did it sufficiently train personnel to detect or respond to known social engineering techniques such as vishing. The failure to implement these basic, industry-standard protections enabled attackers to bypass security and gain access to sensitive data.

261. In the vishing attack, Coforge employees granted a password reset to a caller impersonating an internal Caesars employee without verifying the caller's identity. This enabled cybercriminals to gain unauthorized access to systems containing consumer PII.

262. Coforge's conduct was also unfair under the ICFA. First, its lax verification processes and poor employee training, among others, posed a significant risk to highly sensitive PII in violation of public policy as set in the IPIPA. Second, Coforge's conduct was immoral, unethical, oppressive, or unscrupulous as Coforge continued to present itself as a company possessing cybersecurity expertise, profiting from that representation while exposing Plaintiffs' and Subclass Members' data to foreseeable and preventable harm. Third, Coforge's conduct has caused substantial harm to consumers

263. Consequently, Coforge took actions in violation of the IPIPA and ICFA. That is especially true because, despite failing to reasonably protect Illinois Plaintiffs' and the Illinois Subclass's highly sensitive PII, Coforge continued to benefit from the trust and reliance of their business clients and the Plaintiffs whose data they were entrusted to protect. While Coforge profited from their reputations as secure IT vendors, it failed to take the necessary measures to protect that data, leaving Illinois Plaintiffs and the Illinois Subclass at significant and foreseeable

risk of harm.

264. Illinois Plaintiffs' and the Illinois Subclass's highly sensitive PII was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the PII of tens of millions of individuals. Subsequently, the stolen information was posted on the dark web, exposing their PII and putting them at a substantial risk of misuse of their data.

265. Due to Coforge's inadequate security, and the resulting Data Breach, Illinois Plaintiffs and the Illinois Subclass suffered and will continue to suffer significant injuries, including, but not limited to:

a. loss of privacy;

b. misappropriation of their identity, name and likeness;

c. fraud and identity theft from the misuse of their stolen PII;

d. diminution in the value of their PII due to the loss of security, confidentiality, and privacy;

e. lost value of their PII;

f. emotional and mental distress and anguish resulting from the access, theft and posting of their PII;

g. lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and

h. a continued substantial and imminent risk of the misuse of their PII.

266. Illinois Plaintiffs and the Illinois Subclass also remain at heightened risk of future injury because, based upon information and belief, Coforge continues to provide services to Caesars, and Coforge's inability to adopt or comply with security standards to avoid unauthorized access to their PII puts them at continued risk. Without the use of adequate data security, Illinois Plaintiffs and the Illinois Subclass remain at a heightened and substantial risk that their PII will be subject to another data breach.

267. Illinois Plaintiffs and the Illinois Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental

anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

**CLAIM FOR RELIEF IV**

**VIOLATION OF THE MINNESOTA DECEPTIVE TRADE PRACTICES ACT ("MDTPA")**

**MINN. STAT. § 325D.43, *et seq.***

***(On behalf of Minnesota Plaintiffs and the Minnesota Subclass)***

268. Minnesota Plaintiffs, individually and on behalf of the Minnesota Subclass, re-allege and incorporate by reference Paragraphs 1 through 221 as if fully set forth herein.

269. Minnesota affords a cause of action to any person harmed by an entity's use of deceptive trade practices. Minn. Stat. § 325D.45, Subd. 1.

270. Under MDTPA, a "person engages in a deceptive trade practice when, in the course of business, vocation or occupation, the person . . . engaged in (i) unfair methods of competition, or (ii) unfair or unconscionable acts or practices." Minn. Stat. § 325D.44, subd. 1(13).

271. Coforge engaged in unfair and unconscionable practices by failing to implement reasonable data security measures and employee training protocols that would have prevented a known risk of harm from social engineering schemes like vishing.

272. Coforge managed access to Minnesota Plaintiffs' and the Minnesota Subclass's PII. That PII was compromised as a direct result of a vishing attack in which cybercriminals impersonated internal personnel and requested a password reset by phone. Coforge's employees granted this request without verifying the caller's identity, due to inadequate training and absent verification procedures—despite Coforge publicly claiming it implemented "strict access controls and user authentication measures."

273. Coforge publicly represented that it "follows best practices for ensuring robust data security and privacy," "conduct[s] regular audits and penetration testing," and "safeguard[s] sensitive information both in transit and at rest" through "state-of-the-art technologies" like encryption, Data Loss Prevention (DLP), and Database Activity Monitoring (DAM). These

representations were false, unfair, and unconscionable in light of Coforge's failure to prevent such a basic and foreseeable attack.

274. In the vishing attack, Coforge employees granted a password reset to a caller impersonating an internal Caesars employee without verifying the caller's identity. This enabled cybercriminals to gain unauthorized access to systems containing consumer PII.

275. Coforge's failure to implement widely accepted cybersecurity safeguards—such as training employees to detect social engineering schemes and requiring identity verification before resetting credentials—constitutes immoral, unethical, oppressive, and unscrupulous conduct. This conduct caused substantial harm to consumers and was not outweighed by any countervailing benefits. It was, therefore, both unfair and unconscionable under the MDTPA.

276. As a result of those unlawful and unfair business practices, Minnesota Plaintiffs' and the Minnesota Subclass's highly sensitive PII was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where cybercriminals successfully obtained and exfiltrated the PII.

277. Subsequently, the stolen PII was posted on the dark web, exposing individuals and putting them at a substantial risk of misuse.

278. As a direct and proximate result of Coforge's inadequate security and the resulting Data Breach, Plaintiffs suffered significant injuries, including, but not limited to:

a. loss of privacy;

b. misappropriation of their identity, name, and likeness;

c. fraud and identity theft from the misuse of their stolen PII;

d. diminution in the value of their PII due to the loss of security, confidentiality, and privacy;

e. lost value of their PII;

f. emotional and mental distress and anguish resulting from the access, theft, and posting of their PII;

g. lost time, effort, and expense responding to and preventing the threats and harm posed by the Data Breach; and

h. a continued substantial and imminent risk of the misuse of their PII.

279. Minnesota Plaintiffs and the Minnesota Subclass also remain at heightened risk of future injury because, based upon information and belief, Coforge continues to provide services to Caesars, and Coforge's inability to adopt or comply with security standards to avoid unauthorized access to their PII puts them at continued risk. Without the use of adequate data security, they remain at heightened and substantial risk that their PII will be subject to another data breach.

280. Minnesota Plaintiffs and the Minnesota Subclass seek injunctive relief; costs; reasonable and necessary attorneys' fees as Coforge willing engaged in the deceptive practices; and any other relief available by law and to which the court deems proper.

**CLAIM FOR RELIEF V**

**VIOLATION OF N.Y. GEN. BUS. LAW § 349**

**(*On Behalf Of New York Plaintiffs and The New York Subclass*)**

281. New York Plaintiffs, individually and on behalf of the New York Subclass, re-allege and incorporate by reference Paragraphs 1 through 221 as if fully set forth herein.

282. New York General Business Law § 349(a) states, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful." New York courts specifically interpret § 349 "by looking to the definition of deceptive acts and practices under [S]ection 5 of the Federal Trade Commission Act." *New York v. Feldman*, 210 F. Supp. 2d 294, 302 (S.D.N.Y. 2002).

283. Coforge is a "person, firm, corporation or association or agent or employee thereof" within the meaning of N.Y. Gen. Bus. Law § 349(b).

284. At all relevant times, Coforge was engaged in "business," "trade," or "commerce" within the meaning of N.Y. Gen. Bus. Law § 349(a).

285. New York Plaintiffs and New York Subclass members are each a "person" within the meaning of N.Y. Gen. Bus. Law § 349(h).

286. At all relevant times, Coforge engaged in transactions affecting business, trade or commerce and furnishing services in New York, including, but not limited to, the responsibility for overseeing or contributing to the protocols for properly safeguarding New York Plaintiffs' and

New York Subclass members' PII. This includes through Caesars Sportsbook which New York Plaintiffs and Subclass members accessed through their computers or mobiles phone and provided their PII while located in New York.

287. Specifically, Coforge managed access to New York Plaintiffs' and the New York Subclass's PII. That PII was compromised in a vishing attack, wherein cybercriminals impersonated Caesars employees and successfully requested a password reset over the phone. Coforge's personnel failed to verify the requestor's identity due to inadequate internal protocols and employee training—despite Coforge's claims that it used "strict access controls and user authentication measures."

288. Coforge publicly represented that it "follows best practices for ensuring robust data security and privacy for our clients," and "employ[s] state-of-the-art technologies and processes to safeguard sensitive information," including encryption, Data Loss Prevention (DLP), Database Activity Monitoring (DAM), tokenization, anonymization, and "regular audits and penetration testing." It claimed to "continuously monitor[] systems for vulnerabilities" and to "maintain a proactive security posture."

289. These representations were material and created a reasonable expectation that Coforge would adhere to industry-standard cybersecurity practices. In truth, Coforge failed to implement even the most basic security protocols—including verifying caller identity and training employees to resist social engineering attacks. These omissions and failures were unfair and, in light of Coforge's representations, unconscionable under New York law.

290. New York Plaintiffs and members of the New York Subclass transacted with Coforge in New York and provided their PII in the context of obtaining services in New York. They were entitled to rely on Coforge's duty to safeguard that PII using reasonable security measures.

291. Coforge's failure to adopt or comply with standard data protection measures—despite publicly marketing its commitment to best practices and robust safeguards—was immoral, unethical, oppressive, and unscrupulous. It caused substantial injury to New York Plaintiffs and the New York Subclass and was not reasonably avoidable or outweighed by countervailing

benefits.

292. Consequently, Coforge engaged in acts and practices that violated N.Y. Gen. Bus. Law § 349.

293. Coforge's unlawful, unfair and deceptive acts and practices affected the public interest and consumers at large, including the millions of New Yorkers affected by the Data Breach.

294. As a result of those unlawful unfair and deceptive business practices, New York Plaintiffs' and the New York Subclass's highly sensitive and private PII was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers successfully exfiltrated the PII. Subsequently, the stolen PII was posted on the dark web, placing them at significant risk of harm.

295. As a direct and proximate result of Coforge's inadequate security and the resulting Data Breach, the above unlawful practices and acts caused and will continue to cause substantial injuries to New York Plaintiffs and New York Subclass members that they could not reasonably avoid, including, but not limited to:

a. loss of privacy;

b. misappropriation of their identity, name, and likeness;

c. fraud and identity theft from the misuse of their stolen PII;

d. diminution in the value of their PII due to the loss of security, confidentiality, and privacy;

e. lost value of their PII;

f. emotional and mental distress and anguish resulting from the access, theft and posting of their PII;

g. lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and

h. a continued substantial and imminent risk of the misuse of their PII.

296. New York Plaintiffs and the New York Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and

mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonably necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

## VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated individuals, respectfully request the following relief:

(a) An order certifying this case as a class action;

(b) An order appointing Plaintiffs as class representatives;

(c) An order appointing the undersigned counsel as class counsel;

(d) A declaration that Coforge breached its duties to Plaintiffs and Class Members;

(e) A mandatory injunction directing Coforge to adequately safeguard the PII of Plaintiffs and the Class Members hereinafter by implementing improved security procedures and measures;

(f) A mandatory injunction requiring that Coforge provide notice to Plaintiffs and Class Members relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

(g) An order enjoining Coforge from further unfair, deceptive, and unconscionable practices and making untrue statements about the Data Breach and the stolen PII;

(h) An award of nominal damages, compensatory damages, money for significant and reasonable credit monitoring, statutory damages, treble damages, and punitive damages;

(i) An award of pre-judgment and post-judgment interest as allowed by law;

(j) An award of Plaintiffs' attorneys' fees and litigation costs as allowed by law; and

(k) Such other and further relief as this Court may deem just and proper.

## IX. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury as to all issues so triable.

Dated: July 30, 2025

Respectfully submitted,

*/s/ Michael Gayan*

**Michael J. Gayan**
Claggett & Sykes Law Firm
4101 Meadows Lane, Suite 100
Las Vegas, Nevada 89107
Tel. (702) 655-2346
mike@claggettlaw.com

**John A. Yanchunis**
Morgan & Morgan
Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. (813) 223-5505
jyanchunis@ForThePeople.com

**Douglas J. McNamara**
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW, 8th Floor
Washington, D.C. 20005
Tel. (202) 408-4600
dmcnamara@cohenmilstein.com

**Amy Keller**
DiCello Levitt LLP
10 North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
Tel. (312) 214-7900
akeller@dicellolevitt.com

**Jeff Ostrow**
Kopelowitz Ostrow P.A.
1 West Las Olas Blvd, 5th Floor
Ft. Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

**James Pizzirusso**
Hausfeld LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006
Tel. (202) 540-7154
jpizzirusso@hausfeld.com

**Gerard Stranch**
Stranch, Jennings & Garvey, PLLC
223 Rosa L Parks Ave, Suite #200
Nashville, Tennessee 37203
Tel. (615) 254-8801
gstranch@stranchlaw.com

**Gary M. Klinger**
Milberg Coleman Bryson Phillips Grossman, PLLC
227 W. Monroe Street, Suite #2100
Chicago, Illinois 60606
Tel. (866) 252-0878
gklinger@milberg.com

**Sabita J. Soneji**
Tycko & Zavareei LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Tel. (510) 254-6808
ssoneji@tzlegal.com

**Linda P. Nussbaum**
Nussbaum Law Group, P.C.
1133 Avenue of the Americas, 31st Floor
New York, New York 10036
Tel. (917) 438-9189
lnussbaum@nussbaumpc.com

*Counsel for Plaintiffs and the Proposed Classes*

**CERTIFICATE OF SERVICE**

I hereby certify that on the 30th day of July, 2025, a true and correct copy of **AMENDED CLASS ACTION COMPLAINT** was served via the United States District Court's CM/ECF electronic filing system on all counsel of record who have enrolled in this ECF system.

*/s/ Melisa Pytlik*
An Employee of CLAGGETT & SYKES LAW FIRM